ALIBABA CLOUD

阿里云

数据库审计
快速入门

文档版本：20220707

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.C100快速入门 05
2.D100快速入门 07

1.C100快速入门

本文介绍了购买C100数据库审计实例后，通过配置向导快速部署和使用数据库审计服务的具体操作。

前提条件

已购买数据库审计实例。具体操作，请参见购买数据库审计实例。

背景信息

数据库审计服务支持审计自建数据库和阿里云原生数据库。具体支持的数据库类型，请参见支持的数据库类型。

操作步骤

1. 登录数据库审计系统。具体操作，请参见登录数据库审计系统。
2. 添加要审计的数据库。
   i. 在左侧导航栏，选择**资产 > 资产管理**。
   ii. 在**资产管理**页面，单击**添加**。
   iii. 在**添加资产**面板，完成数据库配置。

      推荐您添加RDS型数据库，您可以直接从当前阿里云账号下已开通的RDS实例中选择要添加的实例。

      您也可以添加自建数据库，具体配置描述，请参见ECS自建数据库配置。
   iv. 单击**保存**。
3. 安装流量采集工具（Agent）。

   如果数据库服务器是安装了云助手的云服务器ECS，推荐您通过云助手安装Agent；否则，您需要根据数据库服务器的操作系统类型，下载相应的Agent并手动安装。以下步骤描述了通过云助手安装Agent的方法，关于手动安装Agent，请参见安装Agent。
   i. 在左侧导航栏，选择**系统管理 > Agent管理**。
   ii. 单击**Agent安装**页签。
   iii. 在**通过云助手安装**区域，单击**开始安装**。
   iv. 在**通过云助手安装Agent**对话框，定位到要安装Agent的实例。
   v. 单击该实例**操作**列下的**安装**。
      安装完成后，**Agent状态**显示为**运行中，已连接**。
4. 配置审计规则。

   具体操作，请参见配置审计规则。

   审计规则帮助您发现数据库中的风险。为数据库配置审计规则后，当审计记录命中规则时，会触发告警。
5. 配置告警通知。
   i. 在左侧导航栏，单击**告警通知**。
   ii. 根据需要的告警通知形式，在**短信**或**邮件**页签单击**添加**。

iii. 在**新增告警通知接收配置**面板，完成告警通知配置。

参数	说明
资产	从**资产**列表中，选择您需要添加告警通知的数据库资产。
接收者	新增短信通知时，配置告警接收人的手机号码。新增邮件通知时，配置告警接收人的邮件地址。
告警等级	设置告警的严重等级，支持*低*、*中*和*高*。
告警次数限制	表示24小时内触发同一规则最多发送的告警次数上限，有效范围0~9999。 每天零点告警计数清零。 当该项设置为0时，不限制告警发送的次数。

iv. 单击**保存**。
配置成功后，在产生告警时，您配置的接收者会收到告警通知。

6. 订阅报表。

添加订阅报表任务后，数据库审计系统会定期向您指定的邮箱发送订阅的数据库审计报表，帮助您了解数据库状态。请参见以下步骤，创建订阅任务。

i. 在左侧导航栏，选择**报表中心 > 报表订阅**。

ii. 单击**添加**，在**添加订阅任务**面板，完成订阅任务配置。

订阅任务配置描述，请参见订阅任务配置描述。

iii. 单击**保存**。
成功添加订阅任务。

2.D100快速入门

本文介绍了购买数据库审计D100实例后，如何快速部署和使用数据库审计服务。

背景信息

数据库审计服务支持审计自建数据库和阿里云原生数据库。具体支持的数据库类型，请参见支持的数据库类型。

前提条件

已购买数据库审计D100实例。具体操作，请参见购买数据库审计实例。

操作步骤

1. 登录数据库审计系统。具体操作，请参见登录数据库审计系统。
2. 添加要审计的数据库。
   i. 在左侧导航栏，选择**资产 > 资产管理**。
   ii. 在**资产管理**页面，单击**添加**。
   iii. 在**添加资产**面板，完成数据库配置。

      推荐您添加RDS型数据库，您可以直接从当前阿里云账号下已开通的RDS实例中选择要添加的实例。

      您也可以添加自建数据库，具体配置描述，请参见添加自建数据库。

   iv. 单击**保存**。
3. 安装流量采集工具（Agent）。

   如果数据库服务器是安装了云助手的云服务器ECS，推荐您通过云助手安装Agent；否则，您需要根据数据库服务器的操作系统类型，下载相应的Agent并手动安装。以下步骤描述了通过云助手安装Agent的方法，关于手动安装Agent的具体操作，请参见安装Agent。

   i. 在左侧导航栏，选择**系统配置 > Agent管理**。
   ii. 单击**Agent安装**页签。
   iii. 在**通过云助手安装**区域，单击**开始安装**。
   iv. 在**通过云助手安装Agent**对话框，定位到要安装Agent的实例。

   v. 单击实例**操作**列下的**安装**。
      Agent安装完成后，Agent状态显示为**运行中，已连接**。
4. 配置审计规则。

   具体操作，请参见规则配置。

审计规则帮助您发现数据库中的风险。当审计记录命中审计规则时，会触发告警。

5. 配置告警通知。
   i. 在左侧导航栏，单击**告警通知**。
   ii. 在**风险告警**或**系统告警**页签，单击**添加**。
   iii. 在**添加告警任务**面板，设置告警**名称**、**触发告警的风险级别**、**关联数据库**和**联系人邮箱**。
   iv. 单击**保存**。
   配置成功后，在产生告警时，您的邮箱会收到告警通知。
6. 订阅报表。

   添加订阅报表任务后，数据库审计系统会定期向您指定的邮箱发送订阅的数据库审计报表，帮助您了解数据库状态。请参见以下步骤，创建订阅任务。

   i. 在左侧导航栏，选择**报表中心 > 报表订阅**。
   ii. 在**报表订阅**页面，单击**添加**。
   iii. 在**添加订阅任务**面板，完成订阅任务配置。
   iv. 单击**保存**。
   成功添加订阅任务。